Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

IVAN GRDIĆ

BIOMETRIJA

Završni rad

Pula, 2019.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

IVAN GRDIĆ

BIOMETRIJA

Završni rad

JMBAG: 0135218040, redovan student

Studijski smjer: Informatika

Predmet: Informacijska tehnologija i društvo

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Pula, rujan 2019.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Ivan Grdić, kandidat za prvostupnika informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, 25.rujan 2019 godine

IZJAVA

o korištenju autorskog djela

Ja, Ivan Grdić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom „Biometrija“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 25. rujan 2019

Potpis

_____

SADRŽAJ:

1. Uvod

U ovom završnom radu obradit će se osnovne i najučestalije biometrijske metode. Biometrijske metode predstavljaju metode koje se koriste za jedinstveno prepoznavanje ljudi i temelje se na jednoj ili više osobina i ponašajnih karakteristika. Obradit će se tehnike za priupljanje otiska prsta, geometrije ruke, prepoznavanja lica, provjere glasa, biometrije oka, prepoznavanja potpisa i dinamike tipkanja. Za svaku od bimetrijskih tehnika biti će obješnjeno na koji način funkcioniraju i kako se koriste. Biometrija kao tehnika nastala je iz potrebe sagledane sa sigurnosnog aspekta. Koristi se za pristupe pojedinim sustavima kao produkt sigurnije provjere identiteta za razliku od lozinka, pinova, tokena, kartica i slično.

Isto tako obraditi će se postupak autentifikacije. Prije postojanja biometrijskih metoda također je postojala potreba za provjerom identiteta i to se vršilo preko kartica, lozinka, tokena i pinova. Iako su to i dan danas često korišteni identifikatori, postoji velika mogućnost od gubitka ili krađe istih, te samim time ljudi sebe, pa čak i svoje financijske račune i firme u kojima rade, dovode u opasnost. Gubitak ili krađa tih identifikatora može ljudima loših namjera omogućiti da se nekom sustavu predstave kao vlasnik i da naprave štetu velikih razmjera, bilo to podatkovne, financijske ili neke druge prirode, bez da se zna da to nije napravila osoba koju se smatra krivom. Pošto za svaki štetu netko treba odgovarati, u ovakvom slučaju taj teret pao bi na vlasnika koji je izgubio identifikacijske podatke ili fizičke predmete.

Objasnit će se koje su prijetnje sustavima, koji su nedostaci i rizici koji se javljaju kod autentifikacije, te na koji način biometrija čovjeka ima prednost nad ostalim metodama.

2. Biometrija

Pojam biometrija potječe od grčkih riječi: *bios*=život i *metron*=mjera. Kao što se može pretpostaviti, radi se o mjerenju određenih tjelesnih i ponašajnih karakteristika živih bića, u ovom kontekstu čovjeka. Glede biometrije i biometrijskih identifikacijskih metoda, postoje dvojbe u kojima jedna skupina autora zastupa stajalište da su sve metode idetifikacije u stvari biometrijske te da se radi o klasičnim metodama u novom, digitalnom okruženju, dok druga skupina autora prihvaća suvremene tehnološke mogućnosti koje omogućuju jednostavnije apliciranje identifikacijskih metoda, ali i razvoj novih identifikacijskih metoda temeljenih na identifikacijskim obilježjima koja se nisu mogla prepoznati i korisititi u ranijem, tehnološki limitiranom razdoblju. Neovisno koliko stavovi bili različiti, nema spora da se radi o identifikacijskoj metodi koja je primatno determinirana infomracijsko-digitalnom okruženjem.

Biometrija je grana zanosti i tehnologije kojoj je cilj identificirati osobe ili verificirati identitet osoba na temelju njihovih fizioloških ili ponašajnih karakteristika.[1]

Biometrija se također može definirati i kao matematičko statistička metoda za istraživanje živih bića s obzirom na njihove odnose mjere i broja koji se utvrđuju korištanjem automatiziranih tehničkih sustava mjerenja i registracije.[2]

Suvremena biometarska identifikacija temelji se na fiziološkim osobinama i osobitostima ponašanja određene osobe, tj na prepoznavanju obrazaca ponašanja, odnosno prepoznavanju određenih biometrijskih karakteristika te usporedbi istih s uzorkom pohranjenim u podatkovnom obliku unutar baze podataka određenog sustava. Važno je dodati da je osnovni uvijet za provedbu biometrijske identifikacije mogućnost da se tjelesne i ponašajne karakteristike mogu koristiti u postupku automatske identifikacije.[3]

Sigurnosni sustavi temeljni na biometrijskim karakteristikama prepoznavanja obično se koriste za kontrolu pristupa. Kroz taj se sustav osoba prvo identificira, a zatim joj se omogućuje pristup i radnje u skladu s prije određenim ovlastima i

[1] Biometrijska verifikacija osoba temeljena na značajkama dlana i lica dobivenim iz video sekvenci – Fratrić, I
[2] Pavišić, B., op. Cit., 555.
[3] Biometrijska identifikacija, Radmilović Ž, str 164.

dužnostima. Taj postupak primjene biometrijskih sustava spada u način provjere identiteta koji se sastoji od verifikacije i autentifikacije.

Prilikom izgradnje ili nabave biometrijskog sustava važno je uzeti u obzir niz drugih pokazatelja biometrijskog sustava, odnosno karakteristika koje su pogodno sredstvo za biometrijsku identifikaciju, kako bismo utvrdili identitet osobe od koje je uzorak dobiven. Te karakteristike moraju zadovoljavati sljedeće uvjete:

- Univerzalnost – mora ju posjedovati svaka osoba
- Jedinstvenost – mora biti kod svake osobe različita
- Stalnost – nesmije biti promjenjiva
- Mogućnost prikupljanja – treba biti lako prikupiva i spremljena u računalo
- Učinkovitost – točnost raspoznavanja uporabom ove karakteristike[4]

[4] Biometrijska verifikacija osoba temeljena na značajkama dlana i lica dobivenim iz video sekvenci – Fratrić, I

3. Autentifikacija

Prolazeći kroz svakodnevni život jednog čovjeka, često se nalazimo u situaciji gdje je potrebno provjeriti svoj ili identitet neke druge osobe, odnosno provjeriti tko je ta osoba. Život je mnogo lakši kada u takvim situacijama možemo pouzdati u sigurnu identifikaciju. Na primjer, povećava sigurnost javnosti tako što pomaže razlikovati dobroćudne članove javnosti od poznatih kriminalaca i drugih prijetnji. Pouzdana identifikacija čini također i financijske i poslovne odnose mnogo sigurnijima i učinkovitijima. U najmanju ruku što će korisnici postati oprezniji i odgovorniji za svoje postupke. Automatizacijom procesa provjere autentičnosti, proširili smo skup velikog broja zadataka koje više ne moramo obavljati mi nego taj dio posla za nas mogu napraviti računala i drugi uređaji i olakšati nam život, te ujedno takvi automatizirani procesi mogu osigurati veću sigurnost, učinkovitost i praktičnost našim životima.

Automatizirana autentifikacija omogućuje prilagodbu načina na koji uređaj reagira na različite ljude te osigurava da taj uređaj pouzdano reagira na ispravan način. U praksi se to odvija kroz dvije odvojene radnje: autentifikaciju i autorizaciju. Prvo što se radi je provjera identiteta osobe sa mehanizmom autentifikacije, te je nakon na redu mehanizam autorizacije koji povezuje odgovarajuće akcije sa identitetom te osobe. Razlika između ta dva mehanizma je važna ako se mijenja pristup na koji sustav treba ponovo djelovati na tu osobu. Na primjer, ako određeni zaposlenik podnese ostavku iz svoje tvrtke, tada računala te tvrtke trebaju trebaju bivšem zaposlemniku onemogućiti pristup resursima tvrtke. Može se reći da nema problema ako računala nastave provjeru autentičnosti tog bivšeg zaposlenika sve dok mu onemogućavaju korištenje sustava tvrtke.

Postoje tri temeljne tehnike ili čimbenika koji se koriste u autentifikacijskim mehanizmima. To su:

- Nešto što znaš (obično se odnosi na lozinku i PIN)
- Nešto što imaš (obično se odnosi na kartica ili token)
- Nešto što jesi (odnosi se na biometriju – mjerenje fizičkih značajki ili ljudskih osobina)

3.1. Nešto što znaš: Lozinka i PIN

Najkorišteniji i najjednostavniji mehanizam provjere autentičnosti u današne doba se vrši preko implementacije lozinki i osobnih identifikacijskih brojeva tj. PIN-ova. Prilikom postupka provjere provodi se usporedba niza znakova u atuentifikatoru i verifikatoru. U praksi, sustavi koji koriste lozinke uključuju i koriste različite kriptografske tehnike kako bi se oduprli napadima i doveli sigurnost na najveću moguću razinu. Lozinke su pouzdano funkcionalne sve dok nisu otkrivene potencijalnim zlouporabiteljima bilo to slučajno ili namjerno, ne misleći da mogu biti zloupotrijebljenje. Iako postoje tehničke procedure za smanjenje rizika za nagađanje lozinke od potencijalnog zlouporabitelja ne postoji način da se sprijeći niti jedna osoba niti jedan korisnik od namjernog djeljenja svoje lozine što predstavlja najveći problem.

3.2. Nešto što imaš: Kartica ili Token

Fizički autentifikacijski uređaji, kao što su kartice i lozinke, razvijene su kako bi se eliminirale određene slabosti koje su povezane s lozinkama i sigurnošću. Prednost kartica i tokena je njihova unikatnost ne nemogućnost podjele. Ako osoba da svoju karticu ili token nekoj drugoj odobi, tada će ta osoba biti u mogućnosti koristiti dobiveno, ali isto tako osoba koja je vlasnik neće moći jer u isto vrijeme samo jedna osoba moze imati pristup takvoj jedinstvenoj stvari. Kod potvrde autentičnosti poslužitelj koristi određeni postupak radi provjere koja je dizajnirana za odredeni uredaj koji se koristi, bila to kartica ili token. Međutim ti postupci ne prihvačaju istu vrijednost autentifikatora dva puta. Odgovarajući postupci provjere obično spadaju u dvije kategorije: one koje koriste kriptografiju tajnog ključa i one koje koriste kriptografiju s javnim ključom. Prvi Tokeni za lozniku implementirani su pomoću kriptografije tajnog ključa.

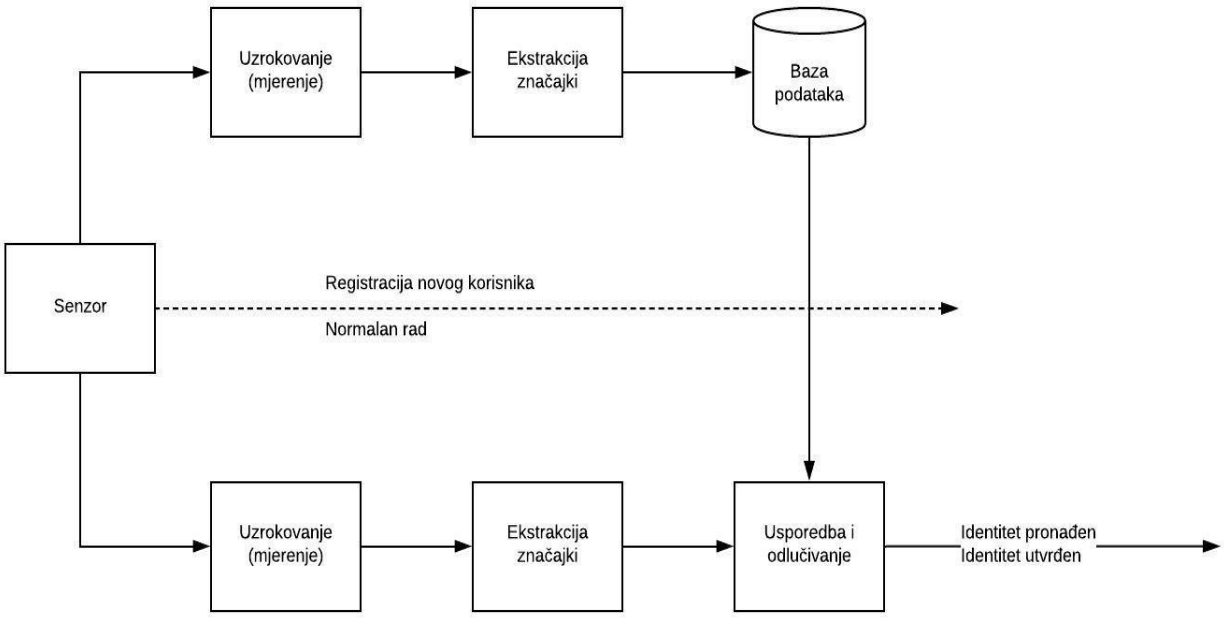
3.3. Nešto što jesi: Biometrija

Biometrijska autentifikacija, predmet ovog rada, temelji se na bilo kojoj automatski mjerljivoj fizičkoj karakteristici ili osobini koja je jedinstvena za svaku osobu. Cilj uobičajenih tehnika biometrijske identifikacije jest pokušaj usklađivanja zapisa otiska prsta, ruke, očiju, lica ili glasa sa zapisima koji su prethodno prikupljeni od te iste osobe i pohranjeni u bazu. Kako bi se mogao izvršiti proces usklađivanja odnosno provjere tih zapisa koriste se dvije metode, a to su identifikacija i verifikacija. Kod identifikacije sustav pokušava utvrditi tko je osoba nad kojom se vrši autentifikacija na način da pretražuje podatke koji se nalaze u bazi. U identifikacijskoj provjeri biometrijski uređaj čita uzorak, obrađuje ga i uspoređuje ga sa svakim zapisom ili predloškom koji se nalaze u bazi podataka. Ovakva vrsta pretraživanja naziva se jedan-na-mnogo(1:N). U ovoj aktivnosti sustav može odrediti da li se uzorak savršeno podudara, te ako nema savršene podudarnosti može izdvojiti zapise prema postotku podudarnosti. Sustavi za identifikaciju su uobičajeni kada je cilj identificirati teroriste ili slične prijetnje na globalnoj razini. Verifikacija se događa u trenutku kada biometrijski sustav pita i pokuša utvrditi da li je to određena osoba, nakon što korisnik tvrdi da je on ta osoba. U zahtijevu za verifikaciju, biometrijski sustav traži unos od strane korisnika te potvrdu da je to uistinu on za kojeg se predstavlja. Taj korisnički unos se uspoređuje sa predloškom u bazi podataka. Isto tako sustav zahtjeva od korisnika i biometrijski uzorak. Zatim se taj uzorak procesuira i vrši se usporedba sa predloškom postojećeg uzorka koji se nalazi u bazi podataka te u slučaju njihove podudarnosti sustav zna da je ta osoba uistinu ona koja bi trebala biti te omogućava daljni tijek radnji ili procesa koje korisnik zahtijeva. Taj cijelokupni postupak se zove verifikacija ili pretraživanje jedan-na-jedan (1:1). U takvim slučajevima za sustav postoje samo dva moguća događaja u kojima ili pronađu podudarnost i verifikacija se uspješno izvrši ili dode do odbijanja.

Na primjer, sustav se može temeljiti na uzimanju otisaka prsta, u tom slučaju taj korisnik mora svoj prst prisloniti na čitać otisaka prilikom prijave u sustav. Čitać će provjeriti otisak koji je pročitan sa čitaćem i usporediti će ga sa otiskom prsta koji je prije prikupljen od korisnika. Ako se otisak koji je dobiven preko čitaća otiska prsta preklapa skoro pa u potpunosti sa postojećim koji se nalazi u bazi sustav zna da je to korisnik koji postoji u tom sustavu te će mu dodjeliti prava pristupa.

4. Proces biometrijske autentifikacije

Svaki proces biometrijske autentifikacije započinje s biometrijskim senzorom neke vrste. Kada se korisnik pokuša prijaviti u sustav kako bi potvrdio svoj identitet, senzor prikuplja biometrijsko očitanje koje je dobiveno preko čitaća otiska, dlana, zjenice i sl. I generira geometrijski predložak iz tog očitanja. Generirani predložak postaje autentikator. Verifikator se temelji na jednom ili više biometrijskih očitanja koja su prethodno prikupljena od korisnika. Nakon što je generiran predložak pokeće se postupak provjere u kojem se vrše mjerenja kojima se utvrđuje potpunost podudaranja autifikatora i verifikatora. Ako sustav odluči da je podudarnost zadovoljena određenim postotkom, sustav autentificira korisnika, inace je sutentifikacija odbijena.



Slika 1.:Shema biometrijskog procesa

5. Prijetnje biometrijskom sustavu

U današnje vrijeme sve je veća potreba za biometrijskim sustavima jer ljudi povremeno pokušavaju pogrešno predstaviti svoje identitete. U prethodnim poglavljima spomenuli smo neke situacije i opisali načine na koje se može pokušati lažno predstaviti i na taj način prevariti sustav. Predstaviti se sustavu kao neka drugi identitet veoma je opasno za osobu čiji je identitet ukraden jer su samim time ugroženi podaci koji mogu biti iskorišteni na razne načine i dovesti osobu u velike probleme bili oni osobni, ekonomski, gospodarski i slično. Sve takve situacije nazivaju se rizici.

5.1. Rizici

U sljedećem poglavlju osvrnuti ćemo se na neke rizike. Rizici predstavljaju različite ciljeve koje bi napadač mogao imati pri pokušaju prevare sustava i provjere autentičnosti. Napadači koji se odvaže na pothvate krađe identieta obično ima veći cilj na umu, kao što je pronevjera veće količine novaca ili hvatanje određene količine robe ili usluga. Kako bi se takve situacije smanjile na minimum, za autentifikacijski sustav, cilj napadača je obično ograničen na jedan od tri opisana: maskiranje, višestruki identiteti ili krađa identiteta.

5.1.1. Maskiranje

Maskiranje spada u klasični, moglo bi se reći i u najpoznatiji rizik za sustav autentifikacije. Kada govorimo o maskiranju, napadać pokušava prevariti ustav. To može postiči na način da pokuša uvjeriti sustav da je on netko drugi, pošto sustav već od prije zna prepoznati pravog vlasnika računa u kojeg napadač želi ući, napadač mora sustav uvjeriti da je on vlasnik iako nije, te ga sustav mora prihvatiti kao neku drugu osobu. Nakon što je napadač uspio prevariti sustav, on je u poziciji da situaciju iskoristi na različite načine. Na primjer, ako napadač postane autentičan isto kao i vlasnik računa sustav mu dozvoljava pristup i korištenje svih podataka koji se nalaze na tom

računu. U takvim slučajevima napadač je u mogućnosti mijenjati podatke u ime vlasnika računa, te ako se kasnije te aktivnosti otkriju pripisuju se vlasniku računa te je upravo on odgovoran za sve promjene cija je narav u većini slučajeva zlonamjerna.

5.1.2. Višestruki identiteti

Postoje sustavi koji donose mnoge pogodnosti građanima, a da bi građani ostvarili te pogodnosti moraju se registrirati u sustav. Za primjer mozemo navesti pružanje socijalnih usluga i različitih benefita građanima slabijeg imovinskog stanja i loše financijske situacije. Da bi građani ostvarili to pravo moraju se sami prijaviti u sustav i potražiti takve usluge. Upravo u takvim situacijama suočavamo se sa problemem kada određeni pojedinci, iz raznih interesa, smatraju da je isplativo i korisno, za iste povlastice, registrirati se dva ili više puta. U konkretnom slučaju korisnik bi se mogao pokušati ragistrirati dva ili više puta tako da benefite koji mu se pružaju može iskoristiti nekoliko puta ili može višestruku registraciju prodati nekom drugom, koji, iz bilo kojeg razloga ne moze ispunjavati uvijete koji bi mu omogućili ispunjavanje uvijeta za socijalne usluge. U takvim situacijama se javlja problem jer sustavi nisu u mogućnosti otkriti višestruke registracije, pa tako jedan te isti korisnik može svaki put koristiti različite identifikacijske podatke i sustav će mu to dozvoliti. Pod tim mislimo na informacije kao što su drugo ime, datum rođenja, mjesto rođenja i slično zajedno s lako dobivenom lažnom dokumentacijom koja sadrži lažna imena. Takvi podaci mogu biti veoma štetni jer postoji određneni broj osoba koje mogu koristiti neke od benefita, te samim time, ako se pojedini korisnik registrira više puta, koristeći različite ne vjerodostojne podatke, onemogućava korištenje tih usluga nekima kojima je to uistinu potrebno.

Praktično i pouzdano riješenje ovakvih problema je korištenje biometrijskih podataka kao dio procesa registracije jer se na taj način sustav ne može zavarati. Ako svaki podnositelj registracije preda biometrijske podatke sustavu, sustav može obaviti provjeru već registriranih korisnika te ako uoći da će doći do podudarnosti biometrijskog podatka između novog podnostelja registracije i svih postojećih registriranih korisnika onemogućava ponovljenu registraciju. Na taj način najlakše je otkloniti probleme višestrukih identiteta i omogućiti, da iz prethodno navedenog

primjera, benefiti koje primaju socijalni slučajevi budu prevedno raspoređeni i podjeljeni.

5.1.3. Krađa identiteta

Krađa identiteta spada u krajnji slučaj rizika autentifikacije kada napadač uspostavi nove račune koji se pripisuju određenoj žrtvi, ali su ovjerene od strane napadača. Prilikom jednostavnog maskiranja, napadač može privremeno preuzeti identitet žrtve u kontekstu sustava koji žrtva već koristi. U krađi identiteta, napadač prikuplja osobne identifikacijske podatke od žrtve i koristi ih za preuzimanje identiteta žrtve u širokom rasponu transakcija i kriminalnih akcija. U ne tipičnoj prijevari napadač otvara račune i predstavlja se kao osoba čije je osobne podatke prikupio prilikom krađe identiteta iako je vrlo uobičajeno i da pljačka postojeće račune.

Iako su agencije za provedbu zakona već počele prikupljati podatke o slučajevima krađe identiteta, mnogi drugi izvori informacija prikazuju da je to sve veći problem. Glavni i suštinski problem u večini slučajeva krađe identiteta je u tome što tipične financijske transakcije potrošača koriste relativno ograničene količine osobnih podataka za provjeru autentičnosti. Tako u situacijama kada je potrošač fizički prisutan tijekom transkacije, trgovac će se vjerojatno osloniti na njegovu osobnu iskaznicu ili slični važeći dokument kako bi potvrdio identitet osobe.[5]

5.2. Pokušaji napada i pogreške

Kada se napadač nađe u situaciji da je suočen sa sustavom autentifikacije, prva i najjednostavnija mogućnost koju razmatra je takozvani pokušaji napada i pogreške i pokušava pronaći način koji povećava mogućnost uspješnosti ove metode. Ne postoji sustav autentifikacije koji nije podložan nekoj vrsti pokušaja napada i pogreške. Uobičajeni napad na lozinke je interaktivni napad u kojem napadač upisjuje lozinku, za koju smatra da bi mogla biti ispravna, jednu za drugom sve dok se ne iscrpi popis

[5] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 10

mogućih lozinki ili sam napadać ne odustane. Čak i u takvim situacijama sustavi su osigurani, tako da se takvim napadima odupiru na način da prate broj neuspjelih pokušaja provjere autentičnosti, a zatim oglašava alarm kada se takve stvari dogode.

5.2.1. Pogađanje lozinke

Već duže vrijeme se koristi heširanje za skrivanje lozinki. Heširanje je kriptografski pristup u kojem je stvarna lozinka promjenjena kako ju eventualni napadač ne bi mogao zlouporabiti.Upravo zbog toga pojavila se drugačija tehnika koja se zove izvanmrežni napad. Ovakva vrsta napada dohvača kopiju kriptografski zaštičene lozinke i koristi računalo kako bi pokusali „probiti“ lozinku. Izvanmrežni napad može uspijeti u dva slučaja: kada pokušavamo „probiti“ lozinku ili kada se koristi riječnićki napad. Izvanmrežni napad može iscrpno provjeriti svaku moguću lozinku uspoređujući njezin heširani ekvivalent sa hešom i na taj način probiti sifriranu lozinku. U riječnićkom napadu, potraga koristi sve riječi na popisu za koje se pretpostavlja da bi mogli biti ekvivalent stvarnoj lozinki. Riječnićki napadi su dovoljno brzi da rječnik može sadržavati i mnoge nevjerojatne riječi za koje se moze reći da nije velika vjerojatnost da su podudarni. U studijama koje se izvode nad datotekama s heširanim lozinkama, rječnici engleskih riječi uspješno su korišteni u rječnićkim napadima kako bi „probili“ između 24,2% i 35% datotečnih lozinki, a to je veoma velik postotak za takav tip metode.

5.2.2. Tokeni i pametne kartice

Uređaji za provjeru autentičnosti takoder su meta interaktivnih i izvanmrežnih napada iako je vjerojatnost uspjeha menogo mala. Interaktivni napad pokušat će generirati legitimnu vrijednost autentifikatora. Vjerojatnost uspjeha napada ovisi o veličini autentifikatora. Budući da autentifikator ima najmanje šest znamenaka, šanse

za uspijeh mogu biti manje od jedan na milijun. Sustav koji ih prima može otkriti interaktivne pokušaje, te tada može oglasiti alarm.

Izvanmrežni napadi na tokene imaju veliku vjerojatnost uspjeha jer ih se ne može otkriti. Cilj takve vrste napada je izvući baznu tajnu pohranjenu na tokenu ili na pametnoj kartici. Prilikom napada isprobavaju se sve prihvatljive vrijednosti za baznu tajnu i testira ih se za presretnute autentifikatore kako bi se utvrdilo da li bi određena vrijednost bazne tajne pokrenula autentifikator. Ovi napadi mogu biti korisni za tokene koji koriste DES ili druge algoritme sa sličnim kratkim duljinama lozinka.

5.2.3. Biometrija

Biometrijski sustavi su mnogo manje podložni napadima pokušaja i pogrešaka nego lozinke i tokeni. Ne postoji način na koji bi napadač uspio prevariti sustav na način da prikaže svoje lice nekoliko puta za redom, a da izgleda kao stvarni vlasnik nekog računa, osim ako su stvarni vlasnik i napadač bliznaci. U tom slučaju će napadač biti u mogućnosti napraviti timski napad na biometrijski sustav, odnosno zavaravati biometrijske senzore, ali realno, za takvo nešto šanse su gotovo zanemarive. Kako bi se ostvarila ovakva vrsta napada, napadač prikuplja nekoliko osoba i traži od njih da se pred senzorom pretvaraju da su vlasnik. Ako je senzor čitač otiska prsta, svaka osoba pokušava sa svakim svojim prstom. Ako je senzor namjenjen prepoznavanju glasa svaki član tima se okreće pokušavajući zvučati kao vlasnik. U teoriji, dovoljno velik tim mogao bi uspijeti, međutim, sustav bi trebao biti u mogućnosti otkriti brojne neuspjele pokušaje i oglasiti alarm prije nego što napadi doista uspiju.

5.3. Ostali napadi

Napadi koji se temelje na pokušajima i pogreškama nisu jedini napadi na koje se napadači mogu osloniti. Postoje i tri dodatna alata koji napadaču omogućavaju praćenje sustava za autentifikaciju: replikacija, krađa i digitalno podvlačenje. Takva

vrsta alata različito djeluje na različite sustave, a djelovanje ovisi o vrsti korištenih autentifikatora.

5.3.1. Replikacija

Kada se dogodi ovakva vrsta napada napadač prilaže kopiju onoga čime se inače vlasnik autentificira. Na Primjer, ako vlasnik za autentifikaciju koristi lozinu i ta je lozinka zapisana na nekom papiru ili fizickom predmetu, napadač može pronaći pisani trag te lozinke te je kopirati i izvršiti napad replikacije, zbog vlastite koristi. Kako se broj korisnika lozinki i broj samih lozinki tijekom prošlog desetlječa povećao, tako se povećao i broj lozinki koje su zapisane, te se isto tako povečala vjerojatnost pronalaska tih lozinki od strane napadača.

Prilikom napada na uređaje kao što su kartice ili tokeni, napad u smislu replikacije znači da je potrebno duplicirati funkcionalnost uređaja, bila to kartica ili token na način da se izdvoji identifikator kartice ili tokena te se taj identifikator koristi preko neke druge kartice ili tokena.[6]

Napadi replikacije na biometrijske podatke imaju cilj oponašati osobna obilježja ili ponašanja koja biometrijski senzor pokušava pročitati. Ovakva vrsta napada često je prikazivana u raznim filmovima. Međutim, u praksi, ovisno o samom senzoru i proceduri koji koristi za verifikaciju, postoje poprilično velike šanse da se biometrijski senzor prevari. Replikacijski napad na biometrijski sustav moguće je izvršiti na dva načina. Korištenjem mimike ili artefakta. Mimika je postupak u kojem napadač pokušava ponašati pokrete na tako sličan način da se predstavi gotovo identično kao i vlasnik. Artefakti su kada napadač pokušava zavarati biomertijski sustav sa na primjer lažnim prstom na kojeg je stavljen otisak vlasnika, koji je unaprijed prikupljen u svrhu prijevare.

[6] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 13

5.3.2. Krađa

U ovakvoj vrsti napada, napadač krade sve fizičke podatke koje korisnik koristi za prijavu. To mogu biti razni fizički predmeti kao što je kartica ili pak obični list papira na kojem je zapisana lozinka. Jedna od pozitivnih stvari kod ovakve vrste krađe je ta što vlasnik lako primjeti da mu nedostaje kartica ili list na kojem je zapisana lozinka i u mogućnosti je intervenirati na način da se spriječi zlonamjerna upotreba ukradenih predmeta. U većini drugih slučajeva korisnik jako teško može na vrijeme otkriti napad. Biomertijska obilježja je jako teško fizički ukrasti.

5.3.3. Digitalna podvala

Ovaj napad koristi činjenicu da su svi podaci za provjeru autentičnosti svedeni na bitove u žici. Ako sustav očekuje određenu vrijednost autentifikatora, jednako tako i napadač može očekivati da će se dogoditi isti taj događaj i u mogućnosti je presresti i pročitati vrijednost kako bi je mogao iskoristiti i predstaviti se kao netko drugi. Takve se procedure događaju kada lozinka putuje u bitovima od klijenta prema poslužitelju i tu je napadać presreće. To je predstavljalo veome ozbiljan problem za promet na internetu sve dok web preglednici nisu počeli koristiti kriptografsku zaštitu. U biometrijskim podacima napad se odvija otipilike na isti način. Napadač započinje napad sa presretanjem najnovijeg biometrijskog očitanja te ukradene podatke podvaljuje kao bi se predstavio kao netko drugi i dobio pristup osobnim podacima korisnika čije je podatke presreo.

6. Mjere obrane

Iako je dizajn sustava provjere autentičnosti često usmjeren na pokušaje i pogreške, osnovne obrambene strategije mogu se koristiti kako bi se opazile sve vrste napada. U mnogim slučajevima obrana se sastoji od kombiniranja jednog faktora autentičnosti s drugim.

6.1. Pokušaj i pogreška

Povečanje veličine tajnih podataka i osjetljivost postupka provjere smatraju se osnovnim strategijama za smanjenje opasnosti od napada. U sustavima koji se temelje na lozinkama, sastoji se od zahtjevanja lozinka koje su duže i teže za pamćenje, dok u isto vrijeme sustav brzo odbija djelomične podudarnosti. S uređajima za provjeru autentičnosti, sastoji se od korištenja dužih tajnih podataka i osigurava da su autentifikatori dugački i dovoljno raznoliki da se odupru offline napadima. Jos jedna od temeljnih strategija je ograničiti broj pretpostavnki: ako netko osigura niz autentifikatora, od kojih niti jedan nije točan, sustav provjere autentičnosti trebao bi oglasiti alarm radi upozorenja da je napad u tijeku. U mnogim slučajevima, sustavi ograničavaju broj uzastopnih neuspjelih pokušaja pod pretpostavnkom da će legitimni korisnik na kraju eventualno poklopiti, dok bi napadač nastavio bezuspješno pokušavati. U biometrijskim sustavima smanjuje se rizik od napada pokušaja i pogrešaka primjenjujuči FAR. Za to se koriste dvije strategije. Prvo, sustav može biti dizajniran na način da koristi informacije iz biometrijskog senzora, što uključuje konstruiranje složenijeg autentifikatora i složeniji postupak provjere. Drugi pristup je prilagođavanje do koje mjere se autentifikator mora podudarati s verifikatorom. Nažalost taj pristup može utjecati na upotrebljivost sustava uzrokujući odbacivanje previše legitimnih korisnika. FAR bilježi pogreške u kojima sustav prihvaća nelegitimne korisnike.[7]

[7] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 15

6.2. Replikacija

Ako se dogodi situacija u kojoj ne postoji način za spriječavanje repliciranja lozinka, postoji nekoliko tehnika koje mogu smanjiti rizik od repliciranja uređaja za provjeru autentičnosti i biometrije. Ako uređaj za provjeru autentičnosti već koristi tajne autentifikatore koji su dovoljno jaki da se odupru pokušajima napada, glavni problem je spriječiti napadake da prikupe tajne podatke. Mjere koje se kriste za obranu od biometrijske replikacije ovise o vrsti podataka koji se prikupljaju. Glavna je strategija uključivanje „živosti“ informacije: mjerenje osobina i ponašanja koja nisu pristna ako napadač predstavlja kopiju biometrijske osobine. Na primjer, neki čitaći otiska prsta su dizajnirani da su osjetljivi na temperaturu prsta ili puls, a sustavi za prepoznavanje lica ili očiju mogu zahtjevati od korisnika da se pomiče dok očitavanje traje.[8]

6.3. Krađa

Krađa se smatra primarnim problemom sa kojim se sučavaju uređaji za provjeru autentičnosti, kao što su lozinka, kartica ili token. Biometrija ne spada u predmet fizičke krađe, jer bi to uključivalo otkidanje dijelova tijela. Na primjer, ako napadač ukrade karticu, njome se nebi trebao moći služiti jer nezna njezinu lozinku i vjerojatno ga nebi uspio pogoditi prije nego bi se oglasnio alarm. Iako krađa pbično nije problem s biometrijskim podacima, neizbježno je pitanje koje se postavlja: „ Što će se dogoditi ako mi odsijeku prst kako bi pokušali pristupiti mom bankovnom računu?“ Problem silčan tome je replikacija i definiran je sličnim tehnikama.[9]

[8] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 15
[9] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 16

7. Biometrijski sustav

Ljudi koriste prirodna osjetila kako bi prepoznali ostale ljude kroz njihove ponašajne i jedinstvene značajke kao što su glas, lice i ostale ljudske karakteristike. Pošto ljudi imaju sposobnost prepoznavati druge ljude, taj sistem moguće je implementirati i u računala i napraviti programsku podršku koja se sastoji od instrukcija koje prikupljaju informacije sa svrhom prepoznavanja ljudi na temelju njihovih jedinstvenih karakteristika. Primarni cilj uporabe biometrijskih sustava je pružiti sigurnost i točnost prepoznavanja identiteta uz veliku pouzdanost, brzinu, praktičnost isto kao i niske troškove.

Postoji nekoliko glavnih razloga zašto biometrijski sustavi postaju značajno popularni:

- Pogodna provjera autentičnosti – pogodna brza i jednostavna autentifikacija omogućava sustavu veću sigunost provjere identiteta za razliku od lozinka, kartica, tokena i ključeva. Sa biometrijom su svi podaci sigurni i ne postoji mogućnost zaborava i gubitka ponašanja ili karakteristika koje se koriste kao identifikatori.
- Povećana potreba za snažnom autentifikacijom – lozinka ili pin mogu lako biti ukradeni. Biometrijski sustavi smanjuju rizik od kompromisa tj, vjerojatnost da napadač može pokazati prikladan identifikator i steći neovlašteni pristup.
- Niski troškovi – tijekom godina poboljšanje u hardverskim i softverskim tehnologijama je rezultiralo smanjenjem cijena biometrijskih autentifikacijskih sustava da budu pristupačne komerijalnoj upotrebi.

8. Biometrijske karakteristike i osobine

Postoji nekoliko ključnih aspekata koji doprinose biometrijskom razvoju. Jedan od njih je robusnost te se odnosi na sposobnost određene biometrijske osobine koja se kontinuirano koristi u biometrijskom sustavu za uspješno automatizirano mjerenje. Drugi vazni aspekat je profiliranost. Profiliranost se odnosi na sposobnost određene biometrijske osobine da se razlikuje od svih ostalih u populaciji svih ostalih korisnika i da je ta razlika mjerljiva.

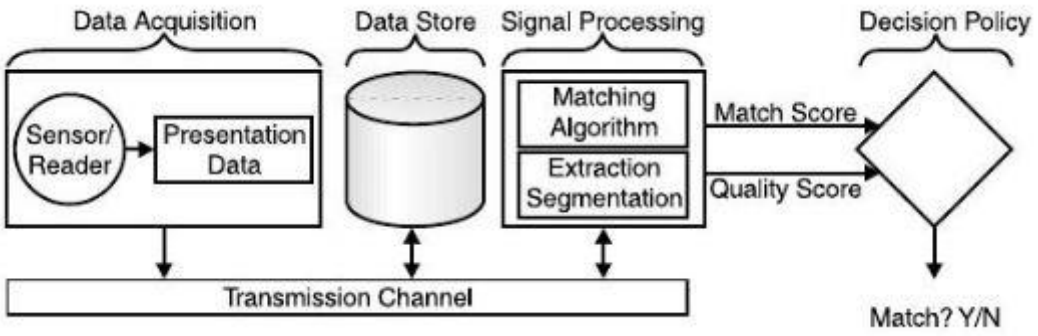
Osobine i karakteristike:

- Genetika – Ovakve nasljedene začajke nasljeđuju se od roditelja. Teoretski neke genetske aspekte, kao što su struktura lica, vrlo je teško promijeniti te to pojedinca čini prepoznatljivim
- Fenotip – Ovakve značajke predstavljaju sve vidljive karakteristike ili osobine nekog bića. Ove se značajke razvijaju u ranim fazama i promatraju se kao zaseban slučaj u genetskom plan razvoja. Omogućavaju veću različitost opće populacije sa određenim genetskim karakteristikama.
- Ponašanje – Ovakve značajke su naučeni ili istrenirani identifikacijski obrasci ponašanja. U teoriji mogu biti promjenjene ili naučene ispočetka.[10]

Sustav koji upravlja tokom prijenosa podataka svih prikupljenih biometrijskih obilježja sastoji se od sljedečih komponenti:

- Prikupljanje podataka – U ovom procesu biometrija je predstavljena sustavu. Sadržaj predstavljaju digitalno snimljeni podaci i prijenos istih u funkcije koje obraduju dobiveni signal. Ako je mjesto na kojem se obrađuju podaci udaljen od mjesta na kojem su prikuljeni, prijenos bi se trebao vršiti enkriptirano
- Kanal za prijenos – Ovaj se postupak odnosi na komunikacijeske kanale između primarnih funkcijskih komponenti. Sustavi se mogu nalaziti unutar samog uređaja ili mogu biti distribuirani.[11]

[10] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 28
[11] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 29



Slika 8.1.: Dijagram komponenata i toka biometrijskog sustava [12]

- Obrada signala – Ovdje se sirovi biometrijski podaci obrađuju radi usporedbe. Sastoji se od segmantacije uzoraka, zatim izoliranja i izdvajanja relevantnih uzoraka iz podataka i stvaranja biometrijskog predloška. Segmentacija je postupak odvajanja relevantnih biometrijskih podataka od pozadinskih informacija. Rezultat ekstrakcije i segmentacije je ocjena kvalitete koja predstavlja kvalitetu uspješno izvađenih značajki. Nakon toga novo stvoreni predložak se pomoću odgovarajučeg algoritma uspoređuje sa jednim ili više referentnih predložaka. Konačni rezultat pokazuje koliko su slični predlošci.
- Odlučivanje – Ovo je posljednji korak u kojem aplikacija razmatra izlaze obrade signala koji se sastoje od ocjene kvalitete i ocjene temeljnosti i donosi konačnu odluku da li je podudaranje predložaka zadovoljavajuće.

[12] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 29

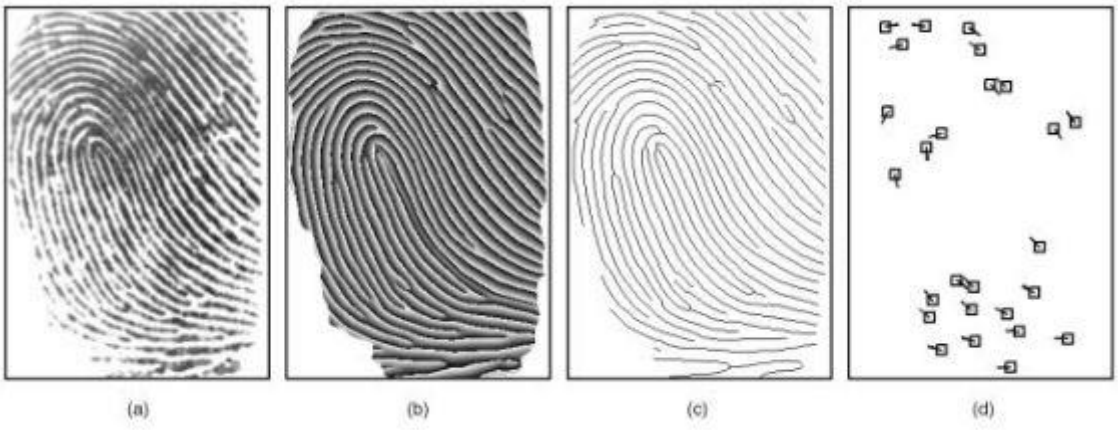
9. Podjela biometrijskih tehnika

9.1. Otisak prsta

Otisak prsta je uzorak koji se sastoji od udubina i izbočina koje se nalaze na jagodici prsta. Svaki pojedinac ima jedinstvene otiske prstiju. Većina sustava za usklađivanje otiska prstiju temelji se na četiri vrste shema reprezentacije otisaka prstiju: siva slika (Bazen et al., 2000), fazna slika (Thebaud, 1999), kosturna slika (Feng, 2006, Hara & Toyama, 2007) i detaljna slika (Ratha i sur., 2000, Bazen i Gerez, 2003). Zbog svoje karakterističnosti, kompaktnosti i kompatibilnosti s karakteristikama koje koriste stručnjaci za ljudske otiske, reprezentacija na temelju detalja postala je najčešće prihvaćena shema predstavljanja otisaka prstiju. [13]

Jedinstvenost otiska prsta isključivo određuju lokalne karakteristike udubina i izbočina i njhihovi međusobn odnosi. Dvije najistaknutije karakteristike izbočine su završetak i bifurkacija. Završetak izbočine definira se kao točka u kojoj se greben naglo završava. Bifurkacija izbočine definirana je kao točka gdje se izbočina spaja sa drugim izbočinama.

Raširena upotreba sustava za prepoznavanje otisaka prstiju u raznim aplikacijama uzrokovala je zabrinutost da se komprimitirani predlošci otiska prsta mogu upotrijebiti za izradu lažnih prstiju.



Slika 9.1.1.: Siva slika(a), fazna slika(b), kostruna slika(c), detaljna slika(d)

[13] Biometrics, Juchen Yang, Fingerprint extraction and recognition

Kao što je spomenuto i ranije, jedinstvenost otiska prsta određena je isključivo lokalnim karakteristikama izbočenja i njihovim međusobnim odnosima. Izbočenja i udubine u otisku prsta izmjenjuju se lokalno sa stalnim smjerom. Zabilježeno je osamnaest različitih obilježja otisaka. Isto tako je identificirano 150 različitih svojstava izbočenja. Karakteristike lokalnih svojstava izbočenja nisu ravnomjerno rasopoređene te većina njih ovisi o kvaliteti otiska prsta. Većina tehnika za vađenje i podudaranje otisaka prstiju ograničava skup obilježja na dvije vrste detalja, a to su završeci izbočenja i bifurkacija izbočenja.[14]

Da bi se izvukli detalji i sve ostale značajke, sustav prolazi kroz nekoliko faza. Prvo se dobiva slika, a zatim se otisak prsta razdvaja od pozadine. Ovaj korak uključuje algoritme detekcije ruba i izbočenja kao što su Fourier-ova dvodimenzionalna transformacija za detekciju okomitih i vodoravnih rubova i Gabor filteri za otkrivanje frekvencije i smjerova. Zatim se područje otiska prsta obrađuje kako vi se rubovi prorijedili na sirinu od 1 pixela i binarno se uspoređuju. Cilj je prikupiti što je više moguće podataa kako bi se odredio položaj izbočine za analizu. Izrađena binarna slika tada se može obraditi kako bi se pronašli detalji. Ovo uključuje Gabor filtara koji se pomiču preko slike. Izračuni pokazuju položaj izbočine i smjer toka, kao i završetak izbočine i promjenu smjera. [15]

9.2. Geometrija ruke

Druga najkorištenija biometrijski identifikator je ruka. Ova vrsta biometrijske tehnologije mjeri mnogo grublje informacije čak i od prošle koja mjeri podatake o prstu. Koristi binarnu sliku za dobivanje svojstva mjerenja poput duljine prsta.

Svaka ruka je jedinstvena. Skeneri za geometriju ruku, poput one koju je napravio RSI[16] mjere duljinu, širinu, debljinu, površinu ruke i četiri prsta. Ove se karakteristike dovoljno razlikuju da se omogući provjera identiteta međutim one nisu dovoljne za pretraživanje identifikacije. Tehnologija koristi CCD digitalni fotoaparat od

[14] Biometrics, Juchen Yang, Fingerprint extraction and recognition
[15] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 62
[16] Recognition Systems, Inc., (RSI) of California, founded in 1986

32.000 piksela za snimanje ručno trodimenzionalnog oblika. Slika RSI sustava prikazana je na slici *9.2.1.: RSI sustav.*

Slika 9.2.1.:RSI Sustav

RSI sustav za izradu slike sastoji se od izvora svjetlosti, kamere, ogledala i ravne površine. Korisnik smješta ruke na ravnu površinu sa dlanom okrenutim prema dolje. Na površini se nalaze pet fizickih djelova koji predstavljaju kontrolne točke koji određuju točno pozicioniranje ruke. Uređaj bilježi dvije slike ruke.

Slika 9.2.2.:Kontrolne točke za pozicioniranje ruke

Nakon snimanja slike, mjesto i veličina ruke određuju se aegmentacijom reflektirane svjetlosti od tamne maskestvorene s rukom zatamnjujući djelove reflektirajuće površine. Druga slika dobiva se za mjerenje profila i debljine ruke. Koristeći samo binarnu sliku ruke i reflektirajuću pozadinu, sustav nije sposoban snimiti ožiljke, izbočine ili čak tetovaže. RSI koristi slike korisnika za izračunavanje duljine širine, debljine i površine četiri prsta koji su bitni; palac se ne koristi. Radi se više od 90 mjerenja i svojstva ruke i prstiju su prikazani predloškom veličine 9 bajtova. Usklađivanje uzoraka uključuje računanje euklidske udaljenosti[17] između napravljenog uzorka i predloška tog identiteta.[18]

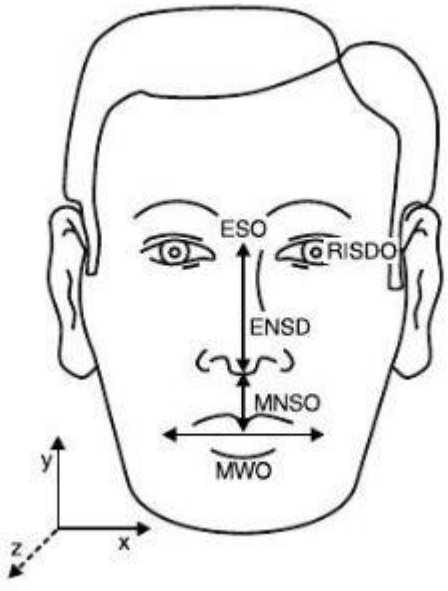
9.3. Prepoznavanje lica

Kao i kod svih bimetrijskih tenika koje se temelje na slici, ispravo otkrivanje, izolacija i registracija subjekta unutar okvira slike je presudan i neophodan korak prije nego što se može izvršiti obrada prepoznavanja. Segmentacija lica je među izazovnijim tehnikama jer postoji velika mogućnost promjene. Položaj kamere, vidno polje i postavke pozadine mogu uvesti znatne razlike u načinu na koji se lice pojavljuje unutar okvira te koliko je lako ili tesko automatski locirati i odvojiti lice od svih djelova koji nisu dio lica. Prepoznavanje lica vrši se prema oblicima i značajkama na slici. Mnoge aplikacije pokušavaju pronaći regije koje liče na lice počevši od sredine prema van. Učinak postupka otkirvanja lica su informacije o lokaciji i registraciji, a sastoje se od minimalnog ograničavajućeg okvira za lice, koordinata očiju, te lokacije dna nosa i središta usta. Učinkovitost otkrivanja lica postala je vrlo pouzdana za pojedinačne slike lica, pa čak i one koje su zakrenute van centra lako će biti prepoznate. Problem nastaje kada se na istoj slici nalazi više lica. Scene u kojima je gužva mogu sadržavati više lica, velike razlike u daljini, kutu kamere i pozi.

Čak i uvjetima koji nisu idealni, mogu se postići zadovoljavajući rezultati ako se softver pravilo podešen i kalibriran, a kamere su strateški postavljene na ciljano okruženje. Uz sve godine usavršavanja i poboljšavanja današnje tehnike najbolje rade u kontroliranim uvjetima. 1996 godine pojavile su se tri klase algoritama: neuronske

[17] Euklidska udaljenost je najkraći razmak između dvije točke u jednom prostoru
[18] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 66

mreže, svojstava lica i lokalna analiza svojstava. Veličine svih predložaka pomalo se razlikuju unutar ova tri glavna pristupa ali općenito su manje od 100 bajtova.

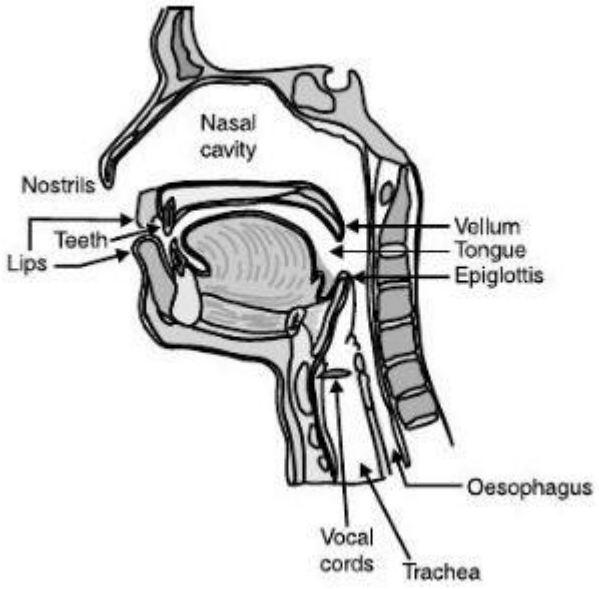


Slika 9.3.1.: Facial recognition

9.4. Provjera glasa

Provjera glasa je biometrijska tehnika koja se sastoji od dvije komponente, fizičke i ponašajne. Osnovna fizička komponenta je glasnica koja se sastoji od oralnih i nosnih dišnih puteva te unutar tih zračnih šupljina nastaju vokalni zvukovi. Fizičke karakteristike zračnih šupljina daju unikate akustične uzorke kod svakog pojedinca. Upravo te karakteristike djeluju kao akustični filter, utječu na ton, visinu i rezonancu ovisno o njihovom obliku, duljini i volumenu. Kretanje, način i izgovor riječi osnova su za ponašajne aspekte glasovne biometrije. Analiza slobodnog govora zasnovana je na modelima govora bez određenog vokabulara, uzima u obzir gramatički kontekst, statistiku učestalosti riječi, idiomatsku upotrebu i druge ritmične i inotacijske aspekte jezika za metriku usporedbu i analizu. Cilj prepoznavanja glasa je razumjeti izgovorene riječi i rečenice tj. sadržaj onoga što se govori. Drugim riječima jedini cilj provjere glasa kao biometrijske tehnike je utvrđivanje identiteta tko govori kako bi potvrdio identitet

pojedinca koristeći svoj glas. Postupak se sastoji od svije procedure. Potrebno je snimiti izgovor, obično preko mikrofona, pa se potom uzorak snimljenog zapisa uspoređuje sa svojstvima priješnje snimljeni uzorak, te ako su ta dva zapisa dovoljno slični korisnik dobiva pravo pristupa ciljanom sustavu.



Slika 9.4.1.: Anatomija stvaranja zvuka

Veličina govornih signala u svakom zapisu je oko 70 ili 80 bajtova, iako informacije koje se mogu naći unutar svakog tog zapisa mogu biti redundantne. U usporedbi sa ostalim biometrijskim tehnikama, prostor za pohranu glasovnih zapisa je nešto veći što zna biti problem u određenim aplikacijama, iako je to u manjim aplikacijama rješeno na način da su ti zapisi definirani jednom riječju pa je isto tako i prostor za porhanu puno manji. Veličina predložaka glasovnih zapisa za autorizaciju zna biti veliki problem kod aplikacija koje imaju velik broj korisnika.Uzorci glasovnih zapisa su valovi sa vremenskom komponentom prikazanom na horizontalnoj osi i glasnočom prikazanom na vertikalnoj osi. Frekvencija vala osnosi se na broj kompletnih ciklua u sekundi u kojima val oscilira. Konventionalni analogni telefoni odašilju elektromagnetske valove koji kruže oko 3kHz. Kada se uzorci zvučnog ili glasovnog vala pretvaraju u digitalni oblik, signali se pojednostavljuju na više malih vremenskih intervala. Digitalni signali su tehnički bolji od analognih jer je kvaliteta mnogo veća, ali isto tako i njhova veličina za pohranu. Prilikom provjere u obzir se

uzima kvaliteta, trajanje, visina zvuka i glasnoča signala te se navedene karakteristike uspoređuju sa unaprijed spremljenim zapisom.[19]

Slika 9.4.2.: Pretvorba glasovnog zapisa

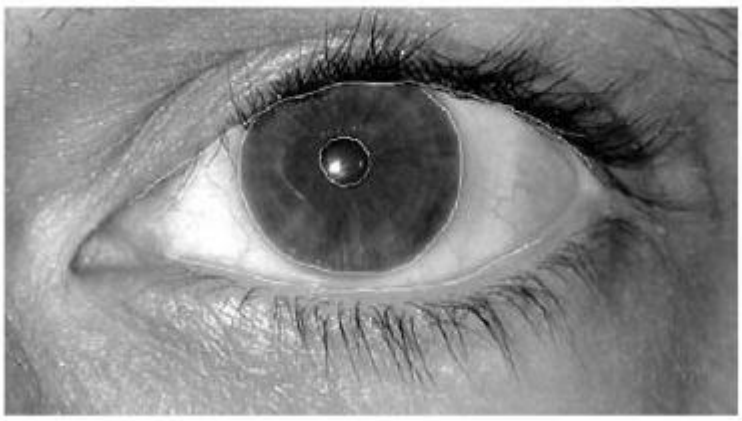
9.5. Biometrija oka

Zamršena priroda ljudskog oka omogućava nam da koristimo dvije najpreciznije biometrijske tehnike. Šarenicu i mrežnicu, koje se nalaze na prednjoj i stražnoj strani oka, definiraju pojedinačno razlikujuće strukture. Šarenica je prsten obojenog tkiva koji okružuje zjenicu. Mrežnica se nalazi na stražnoj strani oka i nije vidljiva, ali sastoji se od različitih značajki. Geometrijski raspored krvnih žila mrežnice je osnova za prepoznavanje na temelju mrežnice.

Šarenica je „okrugla pigmentalna membrana koja okružuje zjenicu oka, a mišići reguliraju količinu svjetlosti koja ulazi u oko.“ Šarenica je sloj ispod rožnice koji je bogat zamršenim uzorcima i teksturama, te je sastavljen od mnogo izbočina i udubina. Tehnologija kojom se radi identifikacija šarenice je akvizicija, analiza i usporedba obrazaca.[20]

Za prepoznavanje šarenice koristi se infracrveno svjetlo i osmišljeno je za rad s kooperativnim subjektima iz neposredne blizine. Neki prilagođeni istraživački sustavi sa specijaliziranim kamerama tvrde da djeluju na znatno dužem operativnom dometu, 5–10 metara dalje od njega.[21] Komercijalni sustavi rade na udaljenosti za fokusiranje od 7 – 17cm. Svaka slika se snima i obrađuje u nijansama crnih boja, a ne u boji te u tom procesu locira i izolira šarenicu. Korekcije veličine i kontrasta provode se na slici kako vi se izbalansiralo prirodno proširenje.

[19] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 83
[20] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 90
[21] Defense Advance Research Projects Agency, “Iris Recognition at a Distance”



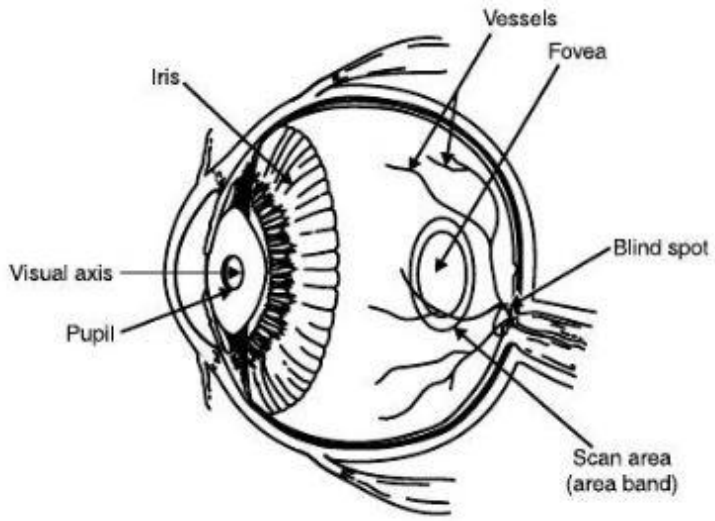
Slika 9.5.1.:Prepoznavanje šarenice

Usporedba dvaju zapisa o šarenici svodi se na niz učinkovitih XOR operacije. To je operacija koja kao ulaze prima dvije vrijednosti, a kao izlaz vrača istinu ili laž, ovisno o tome da li se ulazi podudaraju ili razlikuju.

Uz snimanje šarenice kao biometrijske tehnike za koju se koriste pojedinosti oka, snimati se može i mrežnica u kojoj se identifikacija vrši na temelju uzoraka vena koje se javljaju na stražnjem djelo oka.

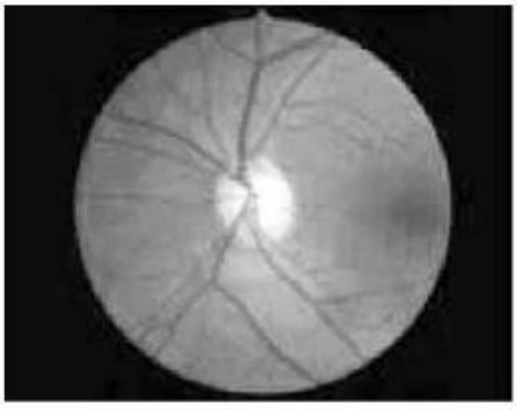
Sekniranje mrežnice provodi se osvjetljivanjem mrežnice infracrvenim svjetlom slabog intenziteta i slikanjem obrazaca koji nastaju u glavnim krvnim žilama. S obzirom da se mrežnica nalazi na stažnjem djelu oka, prilikom snimanja moramo uzeti u obzir da je potreba velika koncentracija i suradnja od korisnika nad kojim se vrši postupak, kako bi se osigurala odgovarajuće osvjetljenje i poravnanje. Tehnologije prepoznavanja mrežnice temelje se na osnovnom krvožilnom sustavu koji je formiran skeniranjem kruga prstenaste regije jer u mrežnici postoje i sitne kapilare i druge zamrštene sitnice. Dobiveni predlošci su veličine 96 bajtova i dobiveni su iz kružne slike koja se pretvori u linearnu strukturu sličnu bar kodu.[22]

[22] Biometrics, John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, 95



Slika 9.5.2.:Prikaz područja skeniranja

Postupak skeniranja mrežnice zahtjeva malu žarišnu udaljenost kako bi se postaupak uspješno izvršio, pa tako i korisnici koji se odluče na taj način prepoznavanja moraju biti spremni surađivati na način koji zahtjeva ova tehnologija. Skeniranje mrežnice se u najviše slučajeva koristi za dobivanje prava pristupa pojedinim prostorijama, odnosno otključavanju vrata. Na taj način se osigurava ulaz u pojedine objekte i kontrolirana područja u kojima se mora znati tko i kada se nalazio u kojoj prostoriji i na kojoj lokaciji.



Slika 9.2.3.: Slika krvnih žila mrežnice

Kada se provodi snimanje korisnici se moraju oko približiti na oko 6cm od skenera, te poravnati pogled prema skeneru. Snimanje se odvija 1 do 2 sekunde.

9.6. Prepoznavanje potpisa

Prepoznavanje potpisa spada u ponašaju biometrijsku tehniku u kojoj se mjere ponašajne značajke. Ponašajne značajke opisuju način na koji subjekt izvršava određenu radnju, odnosno u ovoj biometrijskoj tehnici kako se potpisuje. Verifikacijska tehnologija koja hvata potpis kao potvrdu može se koristiti na bilo kojem mjestu gdje se koristi potpis kao identifikacijska metoda.

Prilikom potpisivanja, funkcija koja je zadužena za provjeru potpisa razmatra značajke samog potpisa i detalje o tome kako se potpis generira. Svaki potpis ima svoja svojstva te ako ga ispisuje ista osoba trebao bi biti približno identičan svaki put kada se generira. Kako bi se obavila provjera da li to uistinu i je tako potrebno je provjeriti informacije od geometriji, zakrivljenosti i obliku pojedinih znakova i cjelovitih riječi. U trenutku generiranja potpisa dobivaju se informacije i o smjeru, brzini kretanja, događajima i olovkama te mjernim podacima tlaka.

Slika 9.6.1.: Interlink ePad digitizers

Interlink ePad digitalizatori su uređaji koji se koriste za prikupljanje digitalnog potpisa. Imaju rezoluciju hvatanja 300ppi (pixels per inch) i izvještavanje 100 puta u sekundi.

9.7. Dinamika tipkanja

Ovakva biometrijska tehnika je nejjeftinija ali njena primjena nije učestala. Posebna je po tome što za razliku od svih ostalih nisu potrebni nikakvi posebni senzori izvan uobičajene tipkovnice. Dinamika pritiska tipke zabilježuje se u potpunosti preko određenog softvera te se s toga ta tehnika može primjeniti na bilo koji sustav u koji korisnik unosi podatke preko tipkovnice. Dinamika pristupa tipke može se koristiti za kontinuirano nadgledanje korisničkog rada nad sustavom ili pak za pojedinačnu provjeru autentičnosti. Jedan od najboljih primjera je ako ovlašteni korisnik koji koristi terminal ostavi upaljeni sustav i udalji se, te nakon toga netko neovlašten nastavi njegov rad, sustav će automatski prepoznati prema dinamici tipkanja da to nije ovlašteni korisnik te će prije nastavka korištenja sustava tražiti ponovnu autenitfikaciju pomoću pina, lozinke ili sličnog. Prisutnost različitog tipkanja tipki po definicji neautorizirano upravljanje može automatski pokrenuti zahtjev za ponovnom provjerom identiteta.

10. Zaključak

Biometrija se svakim danom sve više koristi kao sredstvo autentifikacije u različitim područjima života i kako se naizgled čini, osigurava najveću moguću razinu sigurnosti koju jedan čovjek u današnjem dobu može imati. Iako je sigurnost relativan pojam i ne može biti apsolutna, primjenom biometrije teži se svesti ju na najveću moguću razinu. Biometrija nam omogućava da automatiziranim sustavom promatramo fizičke karakteristike ili ponašanje kako bismo utvrdili nečiji identitet. Njezina najveća prednost je upravo to što nisu potrebne nikakve zaporke, koje predstavljaju velik problem jer ih je lako zaboraviti, izgubili ili razotkriti. Kao što sve ima svoje prednosti i mane tako ima i biometrija. Kako bi se obavila autentifikacija korisnika pomoću biometrije potrebno je imati biometrijske uređaje čija je najveća mana, upravo njihova cijena. Međutim, kad se sve sumira, dovoljna velika poduzeća kojima prihodi omogućavaju da posjeduju neki od biometrijskih uređaja, vjerojatno će se i okrenuti prema takvoj alternativi jer koliko god mislili da je to tek budućnost, takvi sustavi sve više postaju dio današnjice.

Sažetak

Biometrijske tehnike su pouzdane metode koje doprinose autentifikaciji pojedinaca, sa ciljem zaštite ljudskih podataka isto kao i praćenja evidencije njihovog kretanja i pristupanja pojedinim ustanovama. U ne tako dalekim prošlim vremenima, a i dan danas, autentifikacija pojedinaca vršila se preko kartica, lozinka, pinova i tokena, međutim takve metode imaju mnogo nesigurnih točaka i nisu na sigurnosnoj razini kakva je moguća u 21.stoljeću. Upravo radi toga se u sve većem broju implementiraju sustavi biometrije koji sigurnosti pomiću na sljedeću razinu. U ovom radu ukazano je na opasnosti koje se mogu dogoditit prilikom autentifikacije i na koji način korisnici mogu biti oštećeni. Zaključeno je da biometrijska autentifikacija može pružiti najveću pouzdanost i sigurnost, te se očekuje da će postati jedna od najkorištenijih metoda za autentifikaciju.

Abstract

Biometric techniques are reliable methods that contribute to the authentication of individuals, with the aim of protecting human data as well as keeping track of their movement and access to particular institutions. In recent days, and even today, individuals were authenticated through cards, passwords, pins and tokens, however, such methods have many unsafe points and do not have proper security level possible in the 21st century. This is the reason why biometrics systems are being implemented in an increasing number that are move security to the next level. This paper outlines the danger that can occur during authentication and how users can be harmed. It has been concluded that biometic authentication can provide the highest reliability and security, and is expected te become one of the most widely used authentication methods.

Popis literature

Knjiga:

- Fratrić, Ivan (2011) Biometrijska verifikacija osoba temeljena na značajkama dlana i lica dobivenim iz video sekvenci
- Jucheng, Yang (2011) Biometrics
- Raiz, Zahid (2011) Biometric Systems Design and Applications
- Corcoran, Peter (2011) New Approaches to Characterization and Recognition of Faces
- Woodward, D John; Orlans, M Nicholas; Higgins T Peter (2003) Biometrics
- Reid, Paul (2003) Biometrics and Network Security
- Jerčić, Jure (2001) Biometrika i Mendelizam

Članak:

- Boban, Marija; Perišić, Mirjana (2015) Biometrija u sustavu sigurnosi, zaštite i nadzora informacijskih sustava
- Pavišić, B. op. Cit., 555.
- Radmilović, Želimir (2008) Biometrijska identifikacija